Building Trust in PCs

David Grawrock
Security Architect
Desktop Architecture Labs
Intel Corporation

20 January 2000

intel®

Agenda

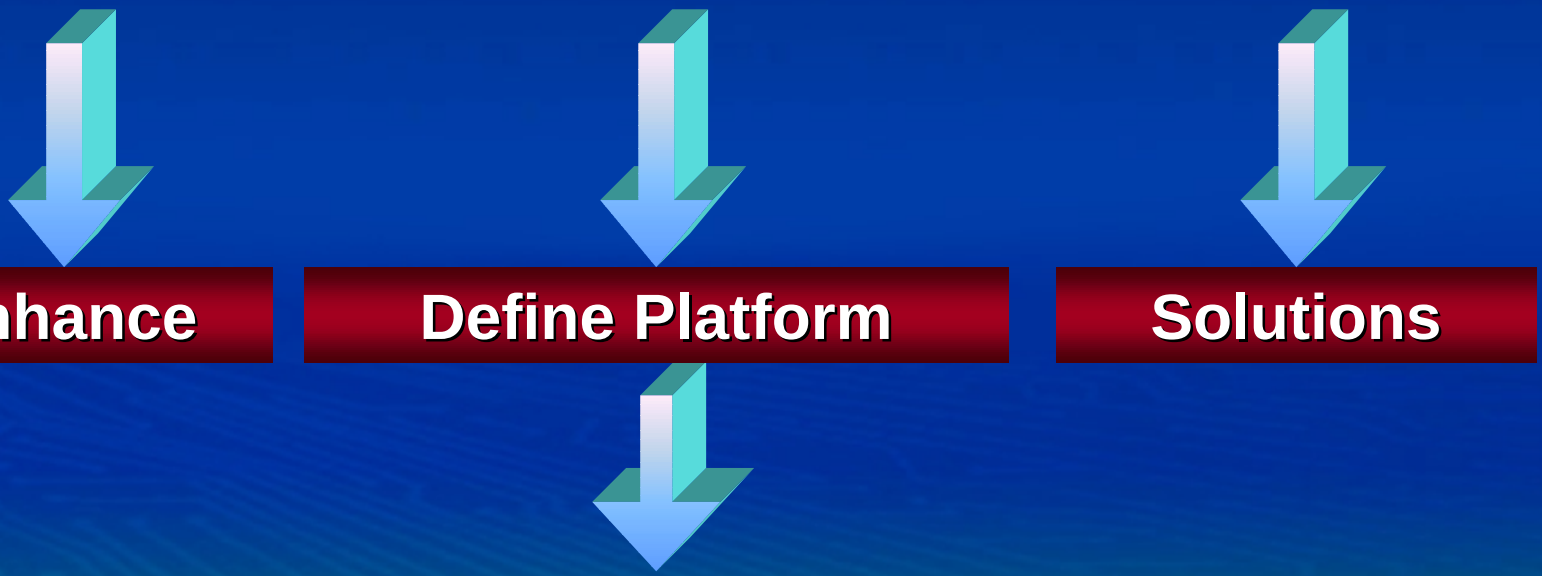
- Trust in the PC
- Feature definitions
- Specifications

Trust Definition

- Users have confidence that the system will behave as they expect it to behave
- Our goal is to increase the users trust in the system

Intel Security Strategy

Technologies	Industry	Products	Services
BIS	TCPA	IPSec NIC	IOS
PAS	PC/SC	Networking	CEO
Random #'s	CDSA	Health Care	IAS
Processor Support		Shiva VPN's	
Algorithms			

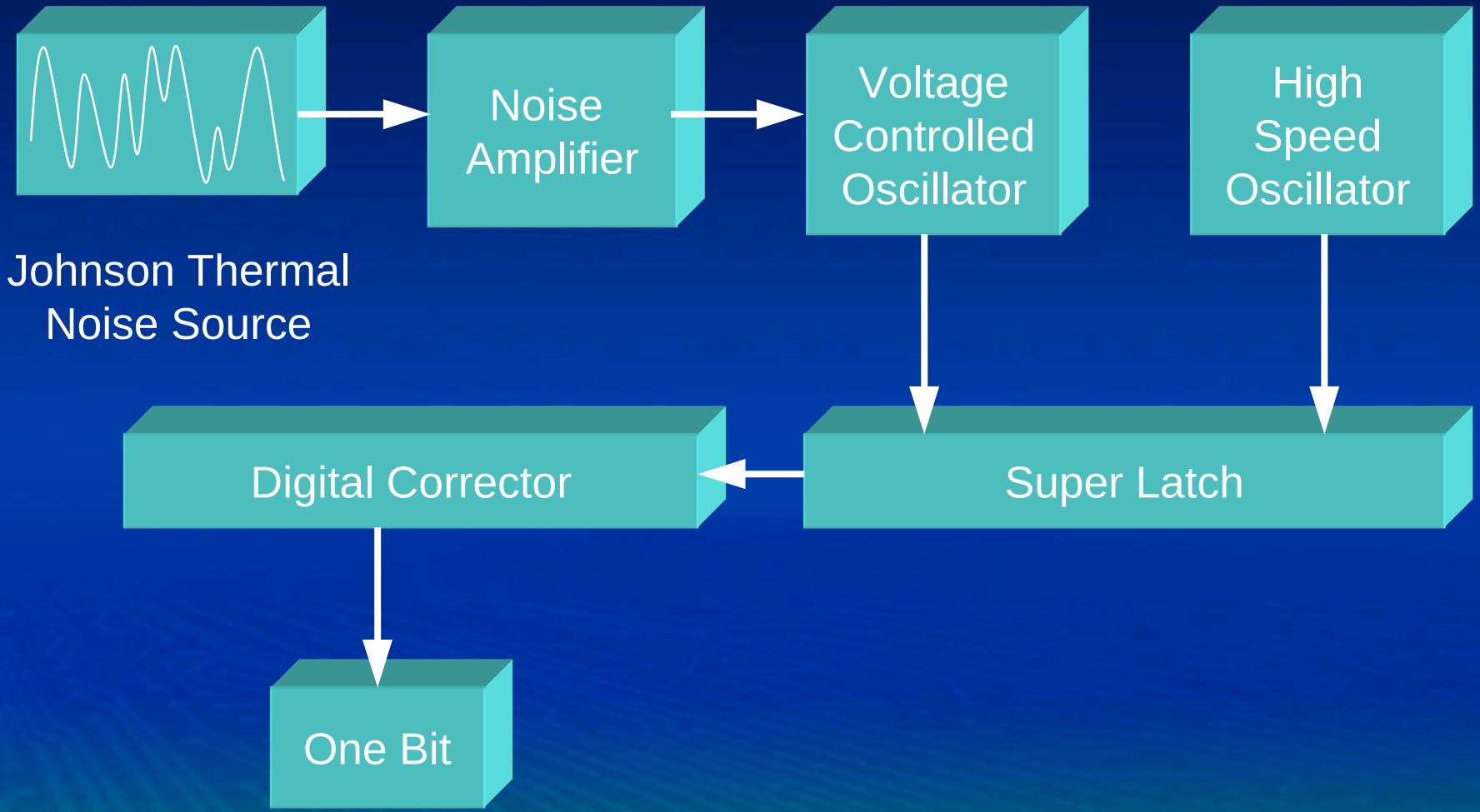


*examples

Random Number Generation

- "Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin."
  - John Von Neumann (1951)
- Are random numbers important?
  - Source for key pair creation
  - Session keys
  - Nonce values

How Does The RNG Work



intel®

RNG Bottom Line

- They really are random
- Products supporting the RNG
  - RSA Crypto J and Crypto C
  - Networks Associates PGP
  - Koal NetDefense
- Details at
  - http://developer.intel.com/design/security/rng/rng.htm
- Use it!!

intel®

Processor Support

- Make current instructions faster
- New types of instructions allow for new types of algorithms
  - Not cryptographically specific instructions

intel®

Faster Itanium™ Instructions

- All instructions work faster because of the architectural design
  - EPIC design
  - Massive resources
- Some instructions receive special help
- Modular exponentiation in particular is faster on Itanium™ processors
  - This makes operations with public and private keys faster

New Instructions

- Itanium™ processor has many enhancements
  - Increased instruction-level parallelism
  - Better management of memory latency
  - Improved branch handling
  - Reduce procedure call overhead
  - Provide massive resources
    - 128 Floating point registers
    - 128 General purpose registers

MMX™ technology

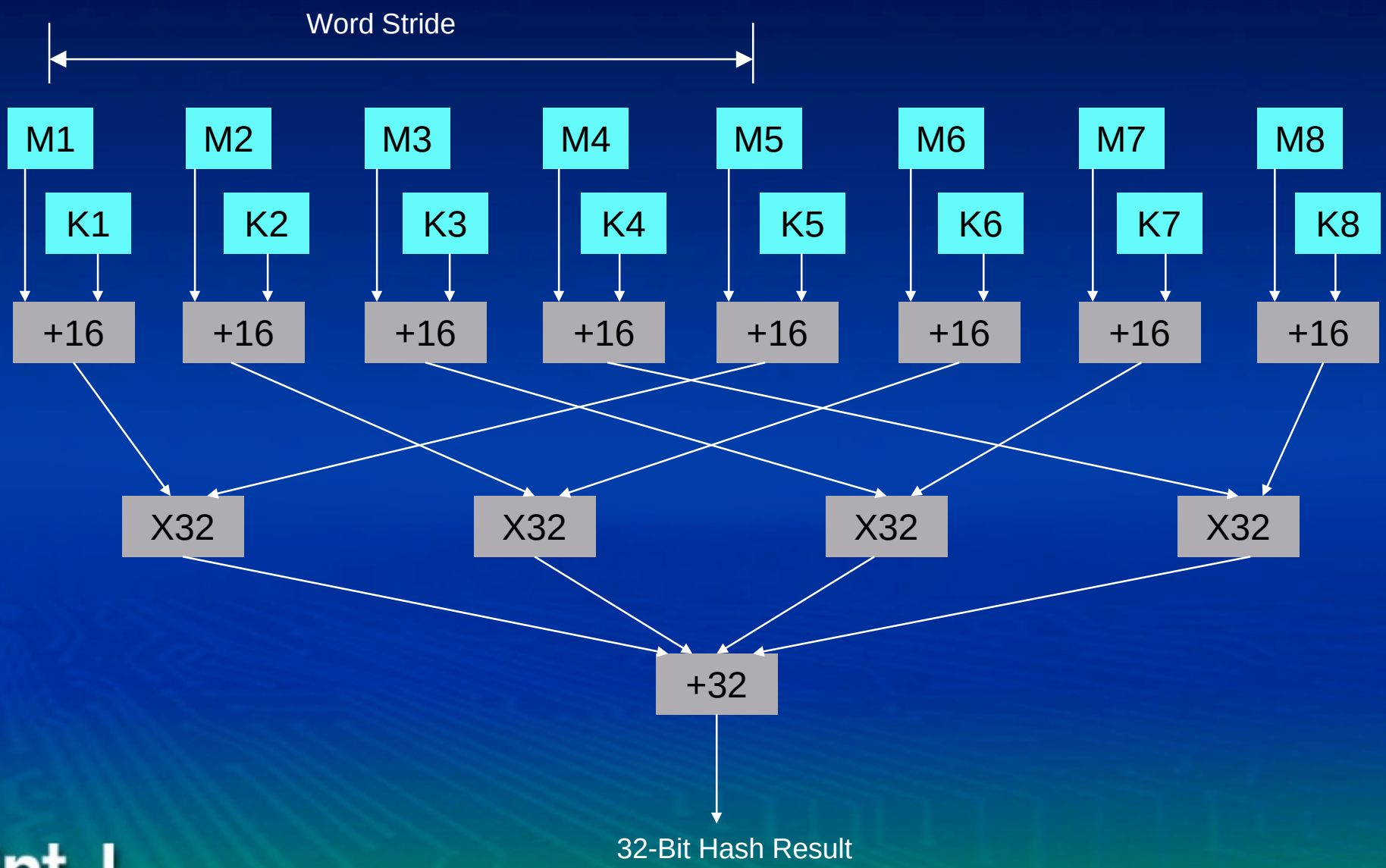
- MMX™ provides new instructions to help improve performance in traditional digital signal processor [DSP] applications
- Typical DSP applications include graphics, audio and voice and telecommunications
- MMX™ is about 4 years old and was first available on some Pentium® processors
- MMX™ isn’t a security technology
  - MMX™ is for graphics, isn’t it?

intel®

MMX™ and UMAC

- UMAC is a new message authentication code
- Uses MMX™ to exploit the SIMD (Single Instruction Multiple Data) architecture
- SIMD is available in Itanium™ processors

UMAC Wordstride



UMAC Locations

- Original paper at Crypto 99
- Web site contains
  - Original paper
  - Source code
  - URL
    - http://www.cs.ucdavis.edu/~rogaway/umac/

New Algorithms

- The Itanium™ processor allows numerous opportunities to create new algorithms
- Download the instruction set and start designing
  - http://developer.intel.com/design/ia64/index.htm?iid=devnav+ia64itn&

Industry Specifications

- Intel works with many industry specification groups
- Some of the specifications that Intel is working on that have a security focus are:
  - TCPA
  - PC/SC
  - BIS
  - PAS

TCPA

- Trusted Computing Platform Alliance
- Defines many of the security primitives of a trusted platform
- Founded by Compaq, Hewlett Packard, IBM, Intel and Microsoft and now including over 80 companies

intel®

TCPA Specification version 1.0

- Proposed System Features
  - Signing
  - Key Generation
  - Random Number Generation
  - Protected Storage / Off sub-system storage (key wrapping)
  - Integrity metrics / challenge
    - BIOS, Option ROM, MBR, OS
  - Tamper resistance

TCPA Status

- Member companies have input into the specification.
- Workgroups address specific areas of concerns
- Join and make your companies voice heard
  - Download membership agreement and bring signed copy to roundtable meeting Thursday evening at the San Jose Hilton Towers, Santa Clara room between 6:00 and 10:00 PM
  - All day meeting on Friday
- Specification in 2000
  - http://www.trustedpc.org

intel®

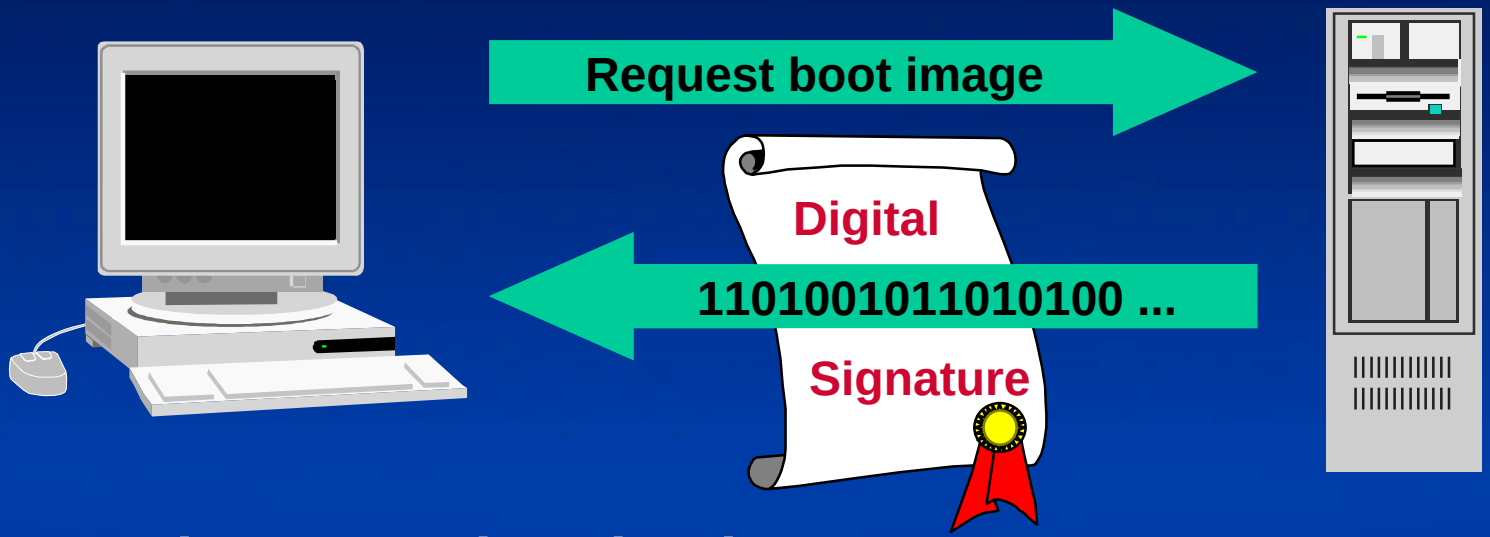
PC/SC

- PC Smart Card specification
- Defines how a PC accesses a smart card
- Companies include:
  - Core members include - Bull, Gemplus, Hewlett-Packard, Intel, Microsoft, Schlumberger, Siemens, Sun, Toshiba

PC/SC Version 2.0

- Version 2.0 includes
  - Support for multiple applications on a smart card
  - Virtual readers
  - Contactless cards
  - Synchronous cards
- Version 2.0 targeted in Q2 2000
- URL
  - http://www.pcscworkgroup.com/

BIS



Boot image authentication

- Digital signature (public key) pre-stored in non volatile memory
- Downloaded program is accompanied by a digital signature (private key)
- BIS in the client performs verification before allowing program execution

BIS Benefits

- Increases assurance of a trusted source for boot images and initial software install
- Increases ability to detect if image was corrupted in transit
- Gives IT more control in using network boot
  - Can associate key pairs with administrators and specific PCs
  - Can reduce operator errors

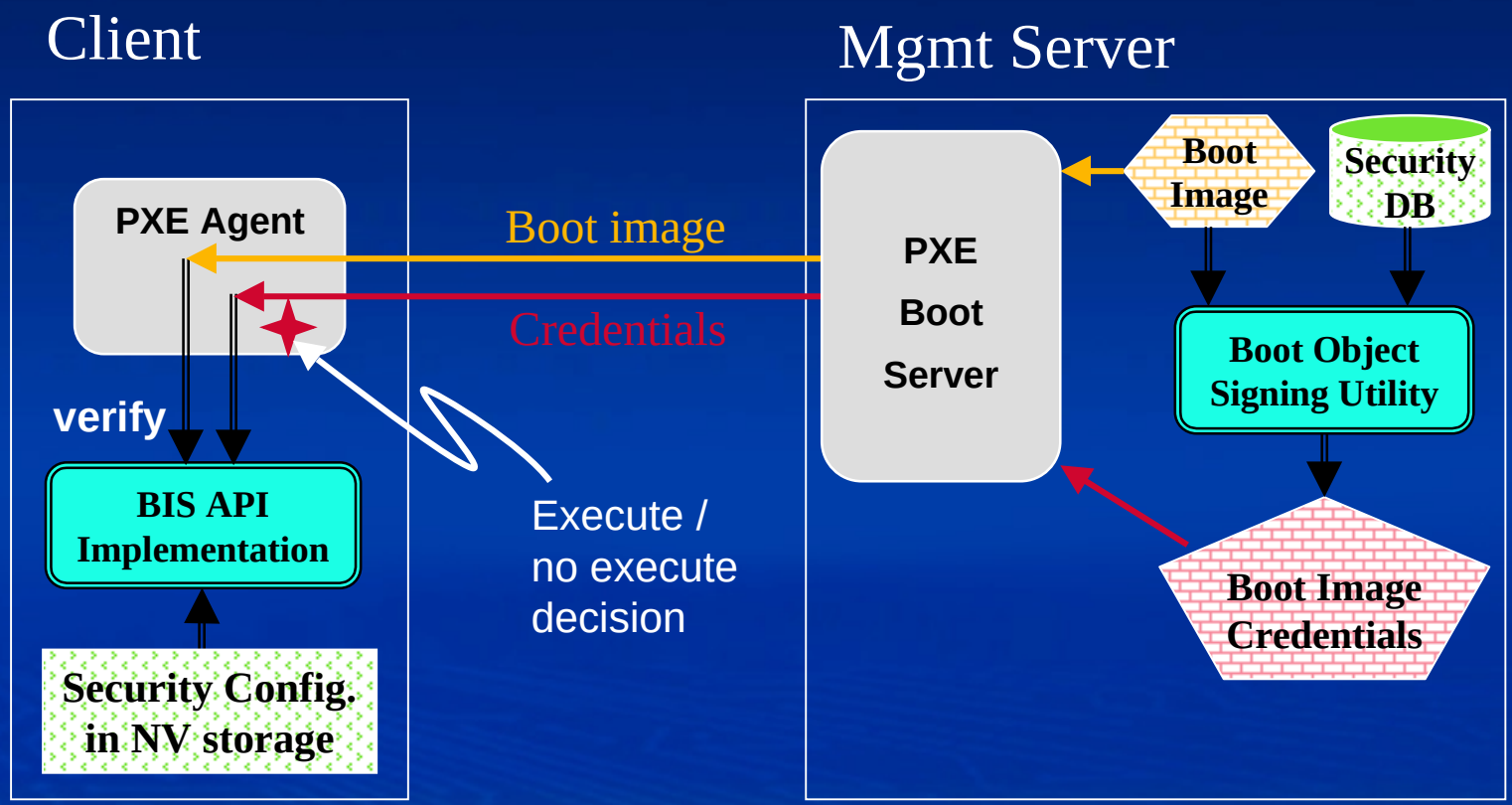
Technical Characteristics

- Standards-based authentication approach
  - Public-key cryptography (PKCS)
  - RSA (512) or DSS (1024) digital signatures (PKCS and P1363)
  - X.509 v3 digital certificates (ITU-T)
  - Signed Manifest Specification, The Open Group
- Focused functionality
- BIS API specification final - December, 1998
- PC2001 Design Guide v. 0.5 refers to BIS as preferred pre-boot authentication scheme

intel®

BIS Usage & Components

Boot image verification



Boot image integrity and authorization

BIS - Summary

- Practical solution to a current problem
- SDK helps simplifies development
- Another step toward better PC security
- URL
  - http://developer.intel.com/design/security/bis/bis.htm

intel®

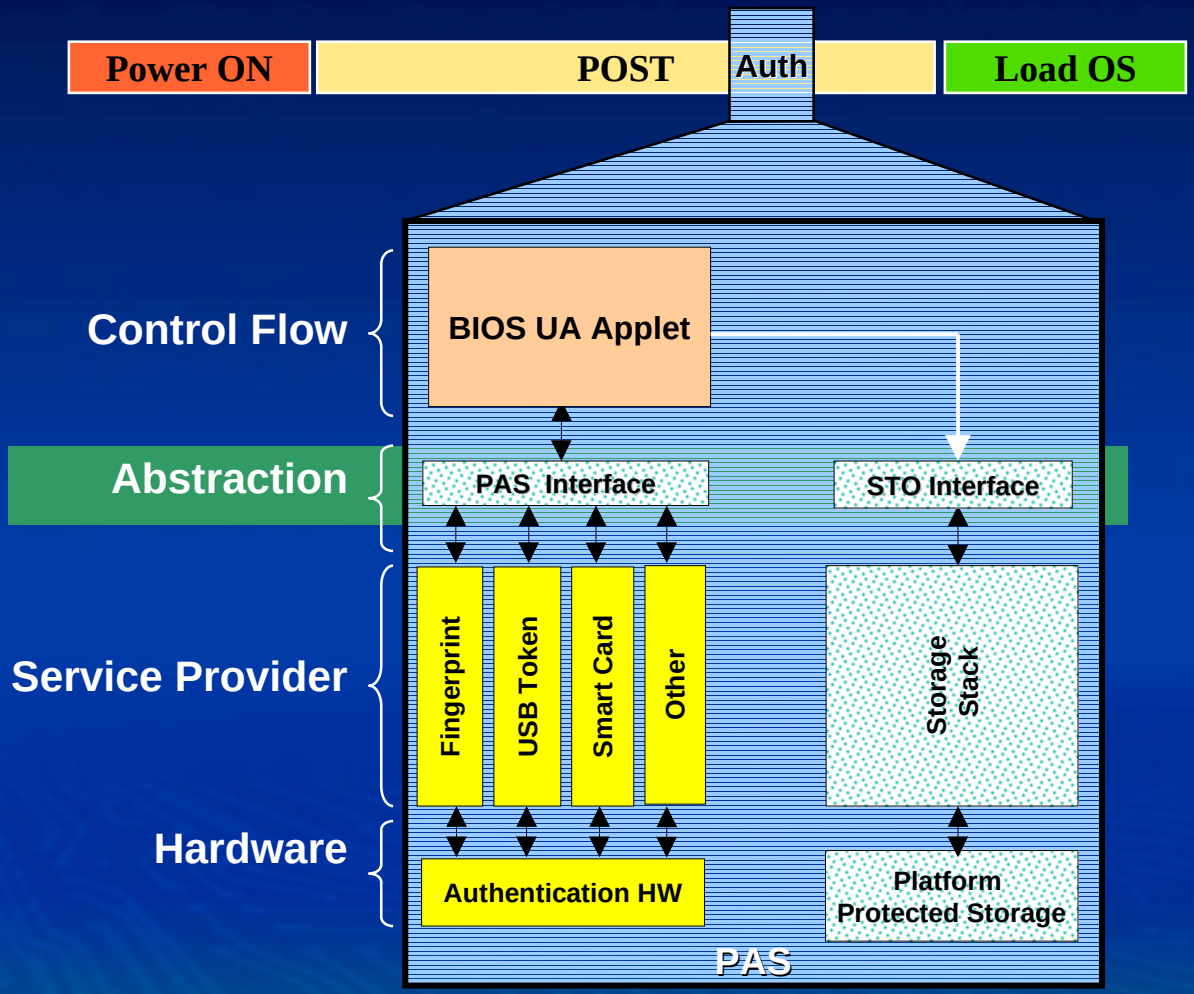
PAS (Pre-OS Authentication Services)

- Mobile PC Theft on the Rise
  - Chubb(98), Safeware(97), Computer World 8/3/98
- Intel Internet Focus Group Studies (IT55 9/98, F1000 9/97)
  - Mobile Security is Greater Concern than Desktop (usually outside the firewall)
  - Solutions Must Address Asset, and Data Security

PAS Solution

- PAS defines pre-OS architecture and services to strengthen user authentication during the “Boot Process”.
  - A method to bind the “User” to their “Platform”
  - Supports multi-factor authentication (Biometrics, Tokens, etc.)
  - Helps deter theft
  - Helps makes a stolen notebook useless
- PAS is designed to be Bus, Token, and BIOS independent
  - Cross-platform, flexible solutions

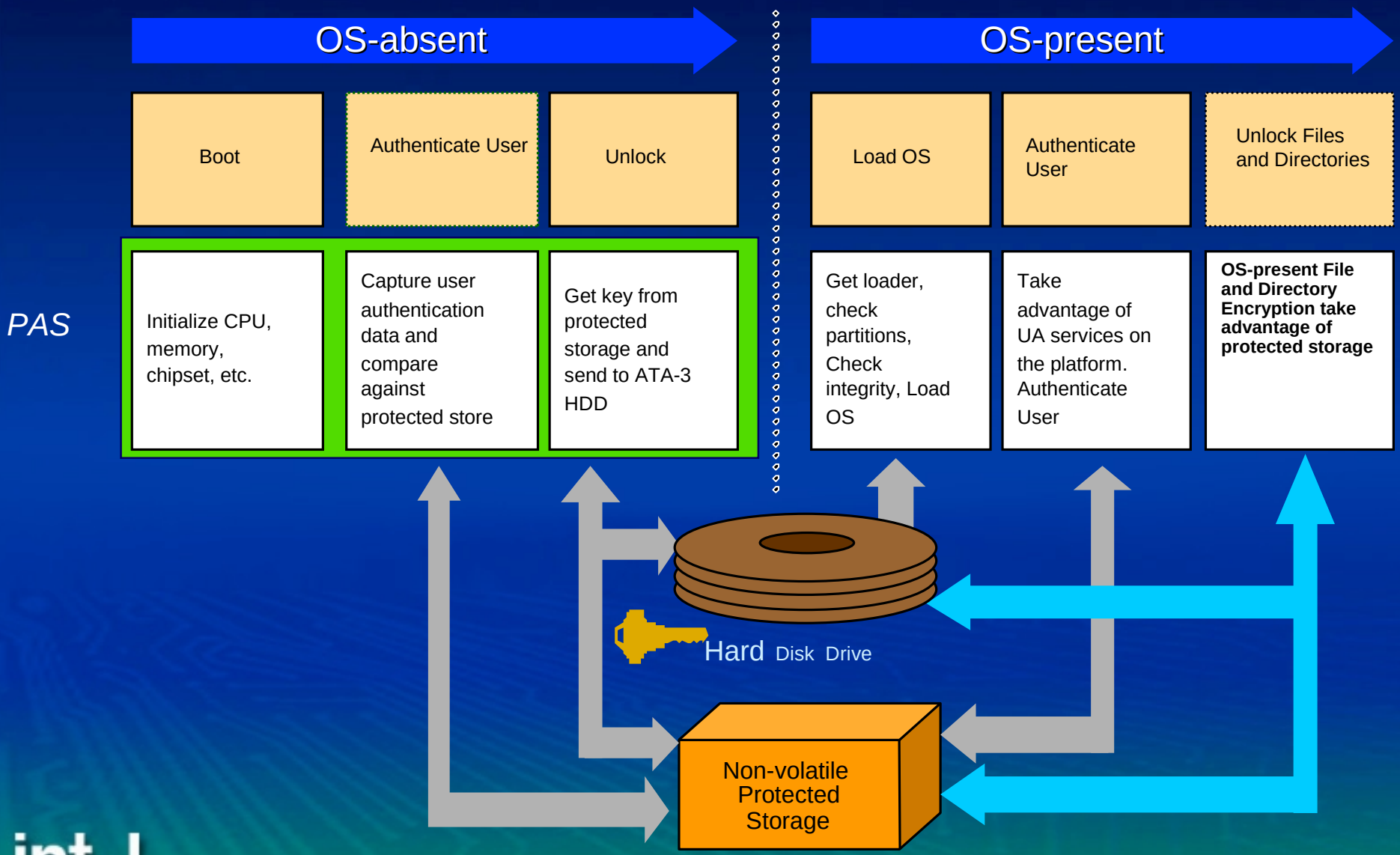
PAS Architecture



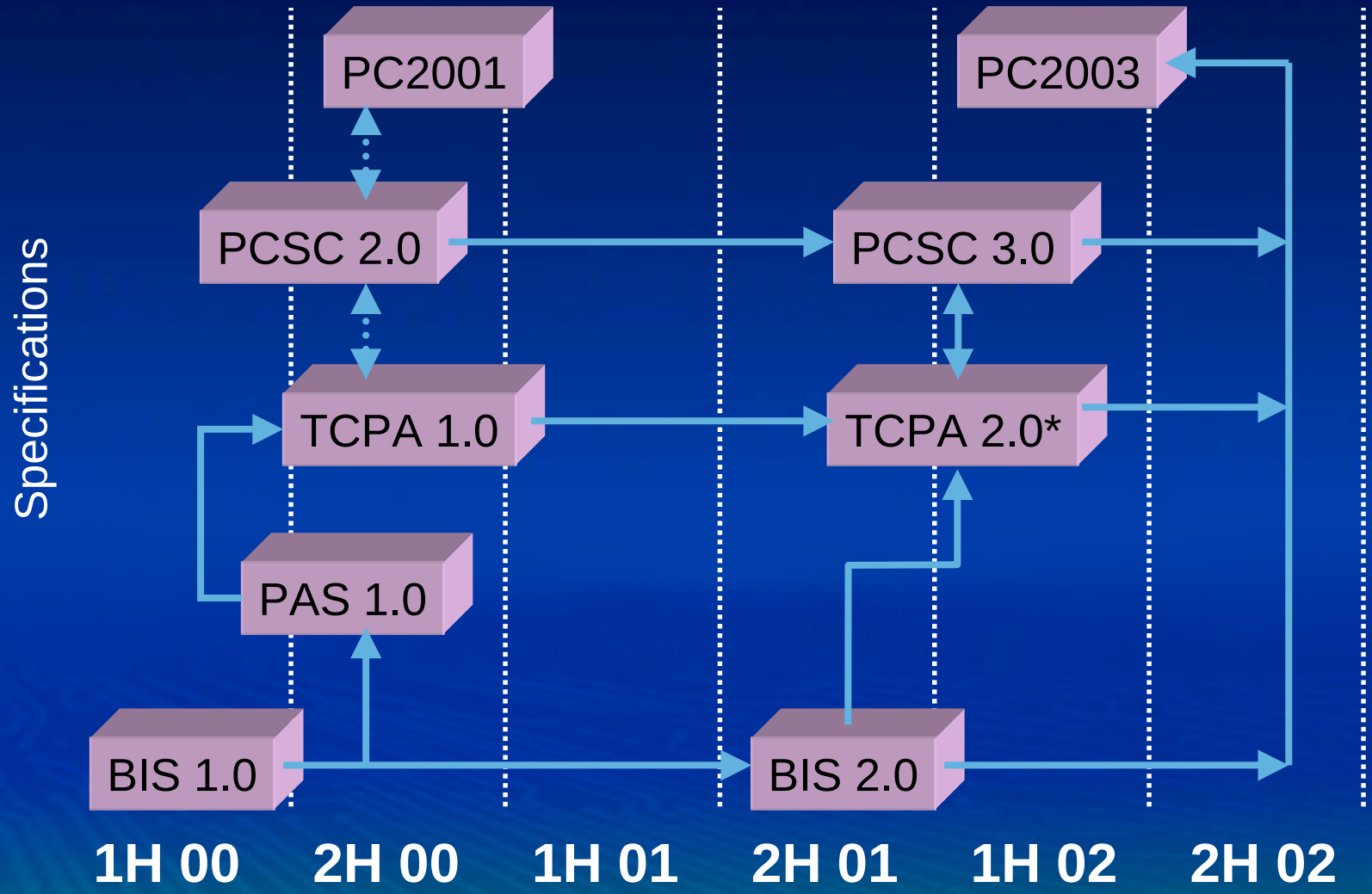
- PAS Defines a pre-OS authentication architecture and interface to token and storage libraries
- Deters theft by not allowing access to unauthorized users.
- BIOS is 1st code to execute
  - Power on, S3, S4, S5
- Authentication Applet executes after sufficient resources are enabled and before OptROM, and Loader
- Must be some protected storage on the platform

intel®

Example PAS Boot Sequence



Roadmap



All dates are estimates only

* 2.0 Has handoff to unnamed standards body

Summary

- Security primitives available now
  - Use the primitives to increase the security of your products
- Faster processors with new features
- New algorithms using the features in unique ways
  - Design new algorithms
- Continued support for industry specifications
  - Help design the specifications
    - Join TCPA
  - Use the specifications when they are available

Thank You!

www.intel.com

intel®